~~25~~

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/738,893	12/15/2000	Yannick Teglia	99-RO-182	2162

23334 7590 06/03/2004

FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI
& BIANCO P.L.
ONE BOCA COMMERCE CENTER
551 NORTHWEST 77TH STREET, SUITE 111
BOCA RATON, FL 33487

EXAMINER	
JACK, TODD M	
ART UNIT	PAPER NUMBER
2133	6

DATE MAILED: 06/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/738,893	**Applicant(s)** TEGLIA, YANNICK
	Examiner Todd M Jack	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

3

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 6 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *1*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 14, 15, 22, and 23 are rejected under 35 U.S.C. 103(a) as being anticipated by Pfab and that which is commonly known in the art.

Claim 1: Pfab teaches a FLASH memory through a data line, connected to a multiplexer, which is connected to the ROM (col. 8, lines 50-57), multiplexer being fed a random number by a random number generator over a data line (col. 8, lines 51-57), and interchanging individual bit lines of the data bus, or by altering the significance of individual data bits (col. 6, lines 54-56). Pfab fails to teach a direct transfer between to memories (taken as literal memory devices). CPUs for transfer units between memories have been obvious to one skilled in the art at the time of the invention was made in order to format the data and direct it to the desired data storage unit.

Claim 2: Further, the encoding or decoding, occurring upon transferring the data, can be performed by a suitable delay, by interchanging individual bit lines of the data bus, or by altering the significance of individual data bits (col. 6, lines 53-57).

Claim 14: Pfab teaches a FLASH memory through a data line, connected to a multiplexer, which is connected to the ROM (col. 8, lines 50-57), multiplexer being fed a random number by a random number generator over a data line (col. 8, lines 51-57), and interchanging individual bit lines of the data bus, or by altering the significance of individual data bits (col. 6, lines 54-56). Pfab fails to teach a direct transfer between to memories (taken as literal memory devices). CPUs for transfer units between memories have been obvious to one skilled in the art at the time of the invention was made in order to format the data and direct it to the desired data storage unit.

Claim 15: Further, the encoding or decoding, occurring upon transferring the data, can be performed by a suitable delay, by interchanging individual bit lines of the data bus, or by altering the significance of individual data bits (col. 6, lines 53-57).

Claim 22: Pfab teaches an encoding module in the CPU and the data memories (col. 6, lines 44-50), interchanging individual bit lines of the data bus (col. 6, lines 53-56), data traffic between the data bus and the CPU is encoded in the encoding module where data traffic consists of Keys from the FLASH memory over the data line transmitted to the encoding module (col. 7, lines 14-20), data memories and the CPU are connected to one another through a data bus (col. 7, lines 41-48), data processing circuit has a CPU as an operating module as well as a plurality of a plurality of data memories (col. 7, lines 41-43), a multiplexer which is connected to a FLASH memory through a data line which can be fed a random number by a random number generator through a data line (col. 6, lines 58-65), the encoding or decoding can be performed in this case by a suitable delay, by interchanging individual bit lines of the data bus, or by altering the significance of individual data bits (col. 6, lines 54-56), and multiplexer being fed a random number by a random number generator over a data line (col. 8, lines 51-57). Pfab fails to teach a direct transfer between to memories (taken as literal memory devices). CPUs for transfer units between memories have been obvious to one skilled in the art at the time of the invention was made in order to format the data and direct it to the desired data storage unit.

Claim 23: Further, Pfab teaches an encoding module, which is provided in the CPU encodes or decodes data traffic between the CPU and the data memories. The encoding and decoding can be performed in this case by a suitable delay, by interchanging individual bit lines of the data bus, or by altering the significance of individual data bits. (col. 6, lines 44-57)

Claims 3, 13, 16, 21 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes and that which is commonly known in the art.

Claim 3: Further, Pfab fails to teach the permutation is defined by the relationship: X = (XO + DIRECTION * PITCH*j) modulo N where PITCH ranges from 0 to N-1, DIRECTION is either 1 or –1, XO ranges from 0 to N-1, and j varies from 0 to N-1. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). A different permutation algorithm is commonly known in the art, it would have been obvious to one skilled in the art at the time of the invention was made to use a particular formula to permute a given incoming data. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a permutation into the algorithm, X= (XO + DIRECTION * PITCH * j) modulo N, using data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements. The data elements are securely transferred in order to allow only authorized individuals to obtain the data.

Claim 13: Further, Pfab fails to teach the permutation is defined by the relationship: X = (XO + DIRECTION * PITCH*j) modulo N where PITCH ranges from 0 to N-1, DIRECTION is either 1 or –1, XO ranges from 0 to N-1, and j varies from 0 to N-1and initializing j and X and transferring step includes the sub-step of repeating N times the steps of: reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index; writing in the second memory the byte that was read from the first memory; and incrementing j and varying X. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need and completing a fundamental subroutine to read-transfer-and write data between memories. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a permutation into the data transfer and to implement a subroutine to allow for the automated transfer of components of memory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

Claim 16: Further, Pfab fails to teach the permutation is defined by the relationship: X = (XO + DIRECTION * PITCH*j) modulo N where PITCH ranges from 0 to N-1, DIRECTION is either 1 or –1, XO ranges from 0 to N-1, and j varies from 0 to N-1. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a permutation into the data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

Claim 21: Claim 13: Further, Pfab fails to teach the permutation is defined by the relationship: X = (XO + DIRECTION * PITCH*j) modulo N where PITCH ranges from 0 to N-1, DIRECTION is either 1 or –1, XO ranges from 0 to N-1, and j varies from 0 to N-

1and initializing j and X and transferring step includes the sub-step of repeating N times the steps of: reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index; writing in the second memory the byte that was read from the first memory; and incrementing j and varying X.. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need and completing a fundamental subroutine to read-transfer-and write data between memories. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a permutation into the data transfer and to implement a subroutine to allow for the automated transfer of components of memory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements

Claim 24: Further, Pfab fails to teach the permutation is defined by the relationship: X = (XO + DIRECTION * PITCH*j) modulo N where PITCH ranges from 0 to N-1, DIRECTION is either 1 or –1, XO ranges from 0 to N-1, and j varies from 0 to N-1. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a permutation into the data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

Claims 4-12 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes.

Claim 4: Further, Pfab fails to teach in the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 5: Further, Pfab fails to teach in the defining step, the value of DIRECTION is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 6: Further, Pfab fails to teach in the defining step, the value of XO is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 7: Further, Pfab fails to teach in the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 8: Further, Pfab fails to teach in the defining step, the value of DIRECTION is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 9: Further, Pfab fails to teach in the defining step, the value of XO is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 10: Further, Pfab fails to teach the defining step, the value of PITCH and the value of XO are chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 11: Further, Pfab fails to teach PITCH and N are mutually prime numbers. Menezes teaches mutually prime numbers, relatively prime, or coprime if gcd(a,b) = 1 (pg. 64, section 2.91). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including mutually prime numbers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to not have degenerate permutation functions, therefore enhancing the security of the data transfer.

Claim 12: Further, Pfab fails to teach N is a prime integer and PITCH is an integer ranging from 1 to N-1. Menezes teaches prime integers (pg. 64, lines 2.92). It is commonly known in the art at the time of the invention that a variable can be defined to be a prime number, and/or an integer ranging between selected values. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including a prime integer and an integer between selected values in the permutation equation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to have a permutation equation which can have an adjusted solution set to allow for changes to occur to enhance security.

Claim 17: Further, Pfab fails to teach in the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 18: Further, Pfab fails to teach in the defining step, the value of DIRECTION is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 19: Further, Pfab fails to teach in the defining step, the value of XO is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

Claim 20: Further, Pfab fails to teach PITCH and N are mutually prime numbers. Menezes teaches mutually prime numbers, relatively prime, or coprime if gcd(a,b) = 1 (pg. 64, section 2.91). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Pfab by including mutually prime numbers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to not have degenerate permutation functions, therefore enhancing the security of the data transfer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 703-305-1027. The examiner can normally be reached on M-Th.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady, can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack
Art Unit 2133

May 12, 2004

CHRISTINE T. TU
Primary Examiner